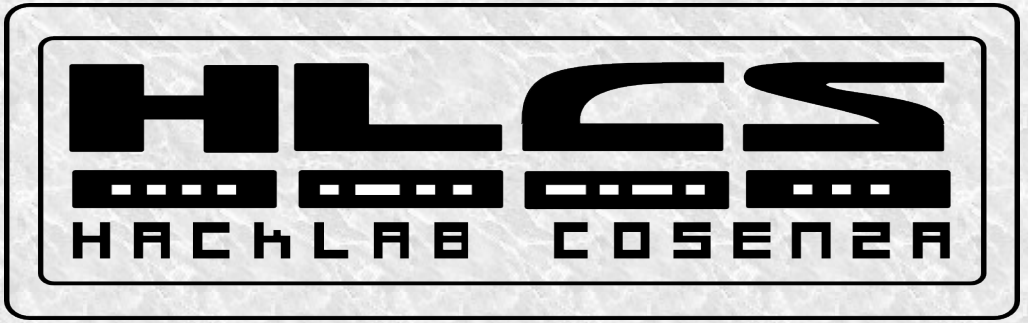


SINGLE-AREA OSPF: messa a punto e troubleshooting

Advanced Networking: Routing & Switching Modulo 3 – Capitolo 5

Copyleft 2014 Hacklab Cosenza (http://hlcs.it)
Released under Creative Commons License 3.0 By-Sa
Cisco name, logo and materials are Copyright Cisco Systems Inc.

Introduzione

- L'OSPF è un popolare protocollo di routing di tipo link state
- Può essere messo a punto in molti modi:
  - elezione del DR/BDR
  - propagazione delle default route
  - fine-tuning delle interfacce (OSPFv2 e OSPFv3)
  - consentire l'autenticazione
- Affronteremo:
  - I comandi di configurazione per implementare queste funzionalità sia per l'IPv4 che per l'Ipv6
  - I comandi utilizzati per risolvere l'OSPFv2 e l'OSPFv3 e le abilità necessarie

Routing

- La raggiungibilità della rete remota è fornita dal router e dagli switch Layer 3 che operano nei layer di distribution e core; questo rende una rete scalabile!
- I router e gli switch Layer 3 conoscono le reti remote in uno dei due modi:
  - Manualmente (routing statico)
  - Dinamicamente (routing dinamico)

Routing Statico

- Un amministratore di rete può configurare manualmente una route statica per raggiungere una determinata rete. Le route statiche non vengono aggiornate automaticamente e devono essere riconfigurate manualmente in qualsiasi momento in cui si apportano o si verificano modifiche alla topologia della rete.
- Ci sono 3 usi principali per il routing statico:
  - In reti piccole, che non ci si aspetta che crescano, fornisce facilità di manutenzione della tabella di routing
  - Routing verso una Stub Network; una stub network è una rete accessibile da un unico percorso, e il router ha un solo vicino.
  - Per l'utilizzo di un percorso predefinito (static default route)

Routing dinamico

- I protocolli di routing permettono ai router di condividere dinamicamente le informazioni sulle reti remote.
- I router che ricevono l'aggiornamento aggiungono queste informazioni alle proprie tabelle di routing.
- I protocolli di routing dinamico, quindi, determinano il percorso migliore.

- VANTAGGI
  - “Meno lavoro” per l'amministratore e per i tecnici
- SVANTAGGI
  - Maggior carico di CPU e maggior utilizzo di link bandwidth

Routing dinamico

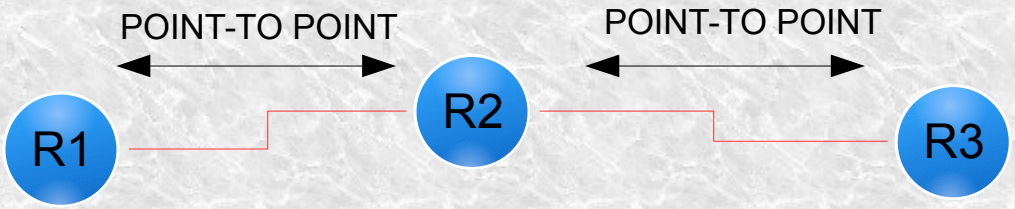
- I protocolli più comunemente utilizzati nel routing dinamico sono:
  - OSPF
  - EIGRP

OSPF: Open Shortest Path First

- L'OSPF è un protocollo di routing di link-state.
- Rappresenta un sostituto del protocollo di routing dinamico RIP (di tipo distance vector) ma con molti vantaggi rispetto al RIP
- CARATTERISTICHE
  - Classless: supporta il VLSM ed il CIDR
  - Efficiente: non necessita di aggiornamenti periodici; le modifiche di routing attivano gli aggiornamenti di routing – il percorso migliore è determinato dall'algoritmo SPF
  - Converge velocemente: propaga rapidamente le modifiche della rete.
  - Scalabile: Funziona bene nelle reti di piccole e di grandi dimensioni
  - Sicuro: Supporta l'autenticazione Message Digest 5 (MD5)

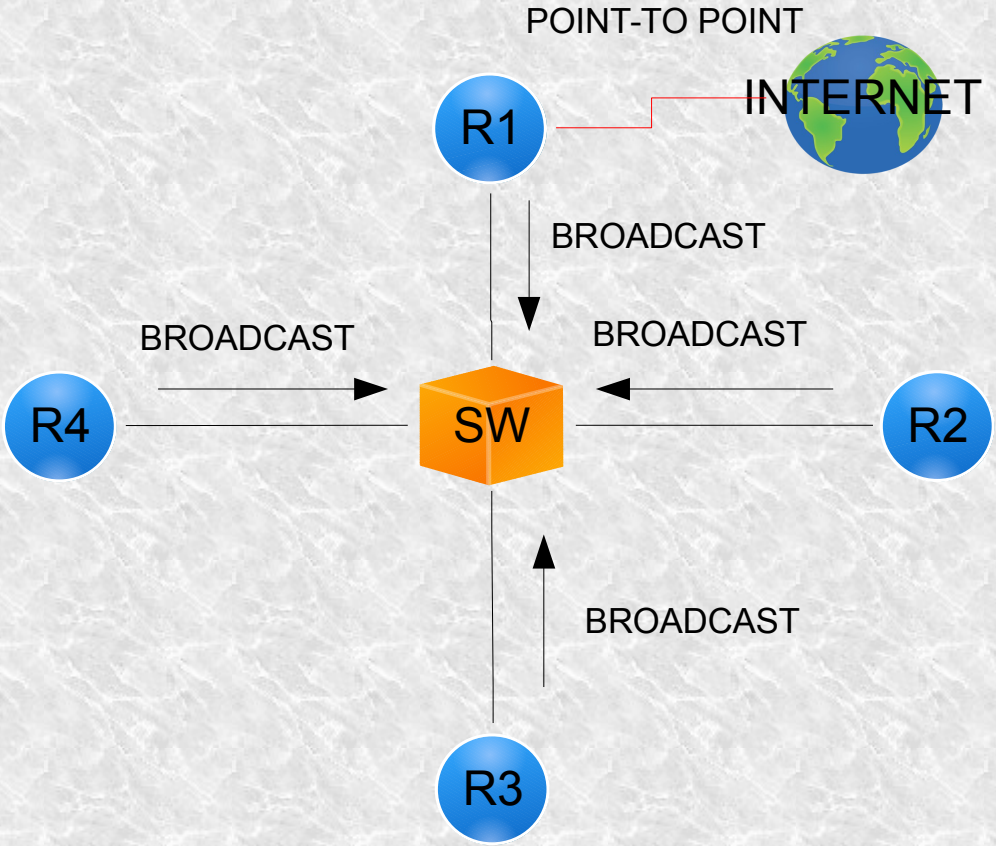
Tipi di rete OSPF
rete 1/5

- Point-to-point: due router connessi tra loro tramite un collegamento comune; nessun altro router è sul collegamento.



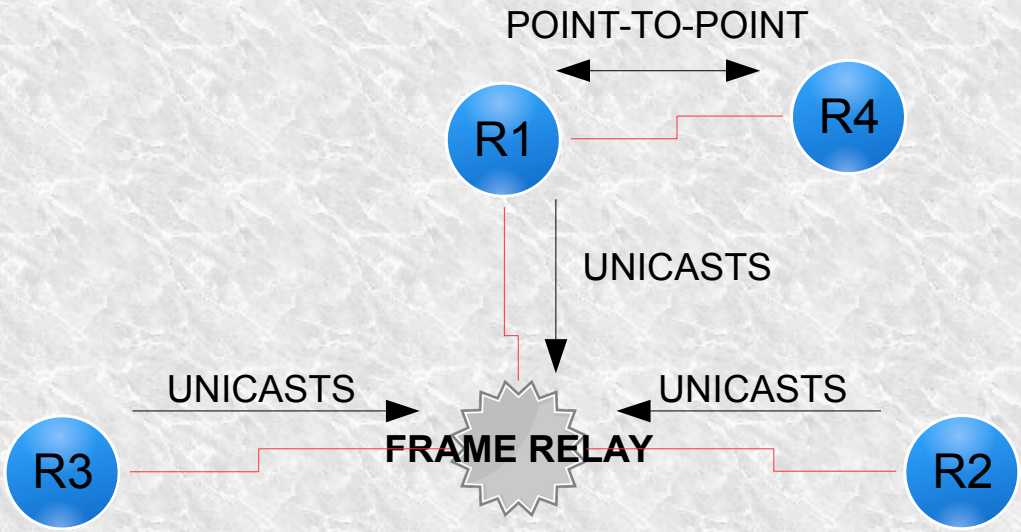
Tipi di rete OSPF
rete 2/5

- Broadcast Multiaccess: diversi router interconnessi tramite una rete Ethernet



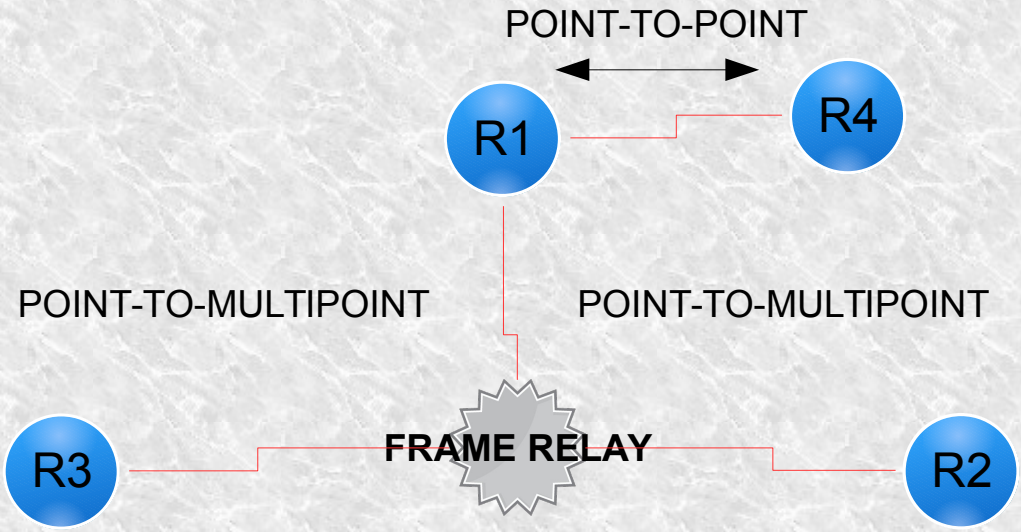
Tipi di rete OSPF
rete 3/5

- Nonbroadcast multiaccess (NBMA): Diversi router interconnessi in una rete che non consentono il broadcast, ad esempio le Frame Relay.



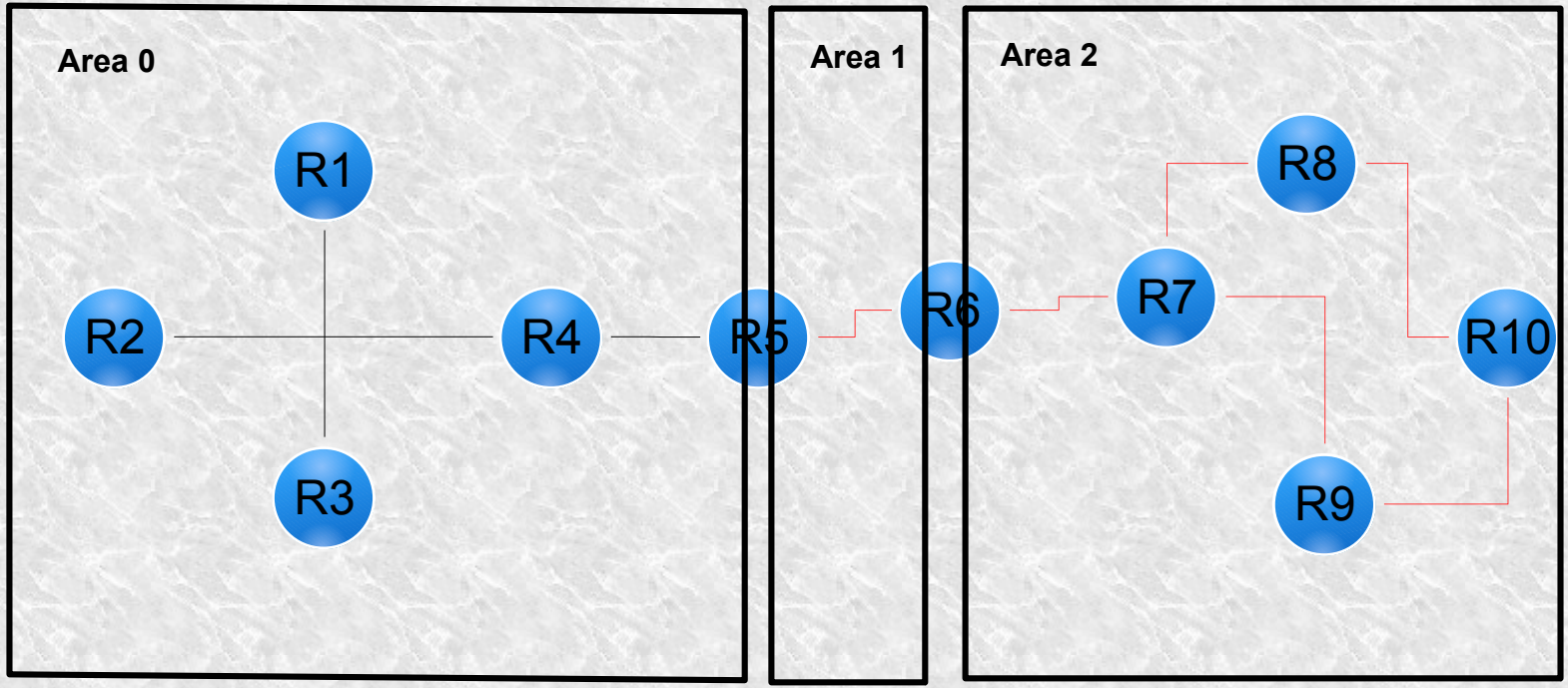
Tipi di rete OSPF
rete 4/5

- Point-to-multipoint: diversi router interconnessi in una topologia hub-and-spoke su una rete NBMA. Spesso utilizzata per collegare i siti filiali (spoke) in un sito centrale (hub)

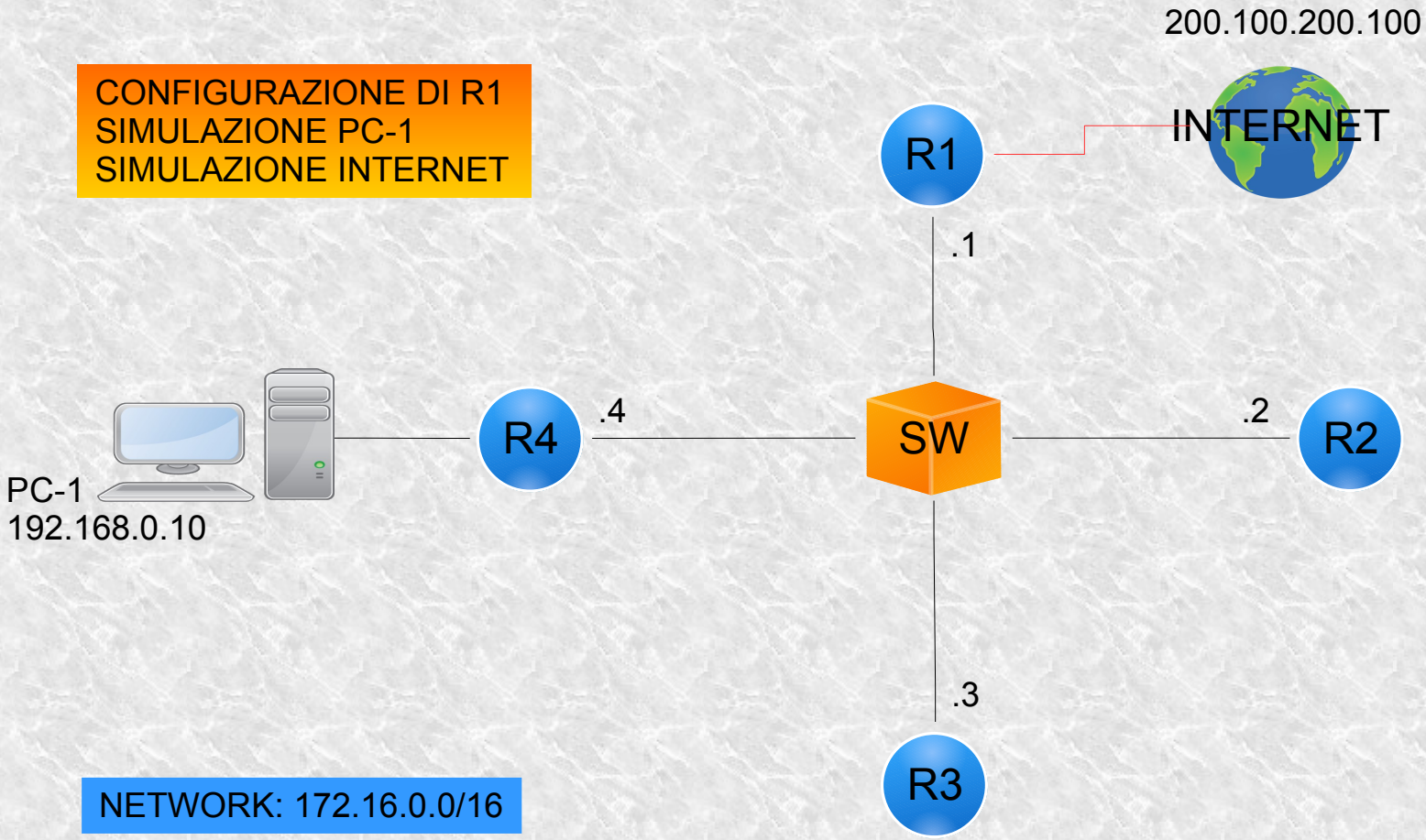


Tipi di rete OSPF
rete 5/5

- Virtual links: rete OSPF speciale utilizzata per interconnettere le aree OSPF lontane dalla backbone area



Topologia di riferimento
(lab su router reali)



Esempio di configurazione Single-Area OSPFv2

- R1(config)#router ospf 1
- R1(config-router)#router-id 1.1.1.1
- R1(config-router)#auto-cost reference-bandwidth 10000
- R1(config-router)#network 172.16.0.0 0.0.255.255 area 0

Comandi di verifica OSPF

- **show ip ospf neighbor**: Comando per verificare che il router ha formato un adiacenza con i suoi neighboring routers. Se il router router ID adiacente non viene visualizzato, o se non mostra di essere in uno stato di FULL, i due router non hanno costituito un OSPF adjacencies.

  R1#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	FULL/DROTHER	00:00:30	172.16.1.2	FastEthernet0/0
3.3.3.3	1	FULL/DROTHER	00:00:31	172.16.1.3	FastEthernet0/0
4.4.4.4	1	FULL/BDR	00:00:39	172.16.1.4	FastEthernet0/0

Comandi di verifica OSPF

- **show ip protocols**: Il comando fornisce un modo rapido per verificare le informazioni di configurazione vitali dell'OSPF. Ciò include il process ID OSPF, il router ID, le reti che il router pubblicizza, i neighbors dai quali il router sta ricevendo gli updates, e la distanza amministrativa di default, che è 110 per l'OSPF.

```
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.10
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.10.4 0.0.0.3 area 0
    192.168.10.8 0.0.0.3 area 0
  Passive Interface(s):
    FastEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.10.5         110      00:04:28
    192.168.10.9         110      00:04:28
    192.168.10.10        110      00:04:28
  Distance: (default is 110)
```

Comandi di verifica OSPFv2

- **show ip ospf**: Il comando viene utilizzato per visualizzare il process ID OSPF ed il router ID, così come le informazioni OSPF SPF e OSPF area information.
- **show ip ospf interface**: Il comando fornisce un elenco dettagliato per ogni interfaccia OSPF-enabled ed è molto utile per determinare se le "network" statements sono state composte correttamente.

Esempio di configurazione Single-Area OSPFv3

- R1(config)#ipv6 unicast-routing
- R1(config)#ipv6 router ospf 10

  %OSPFv3-4-NORTRID: OSPFv3 process 10 could not pick a router-id,please configure manually
- R1(config-rtr)#router-id 1.1.1.1
- R1(config-rtr)#auto-cost reference-bandwidth 10000
- R1(config-rtr)#interface f0/0
- R1(config-if)#ipv6 ospf 10 area 0

Comandi di verifica OSPFv3

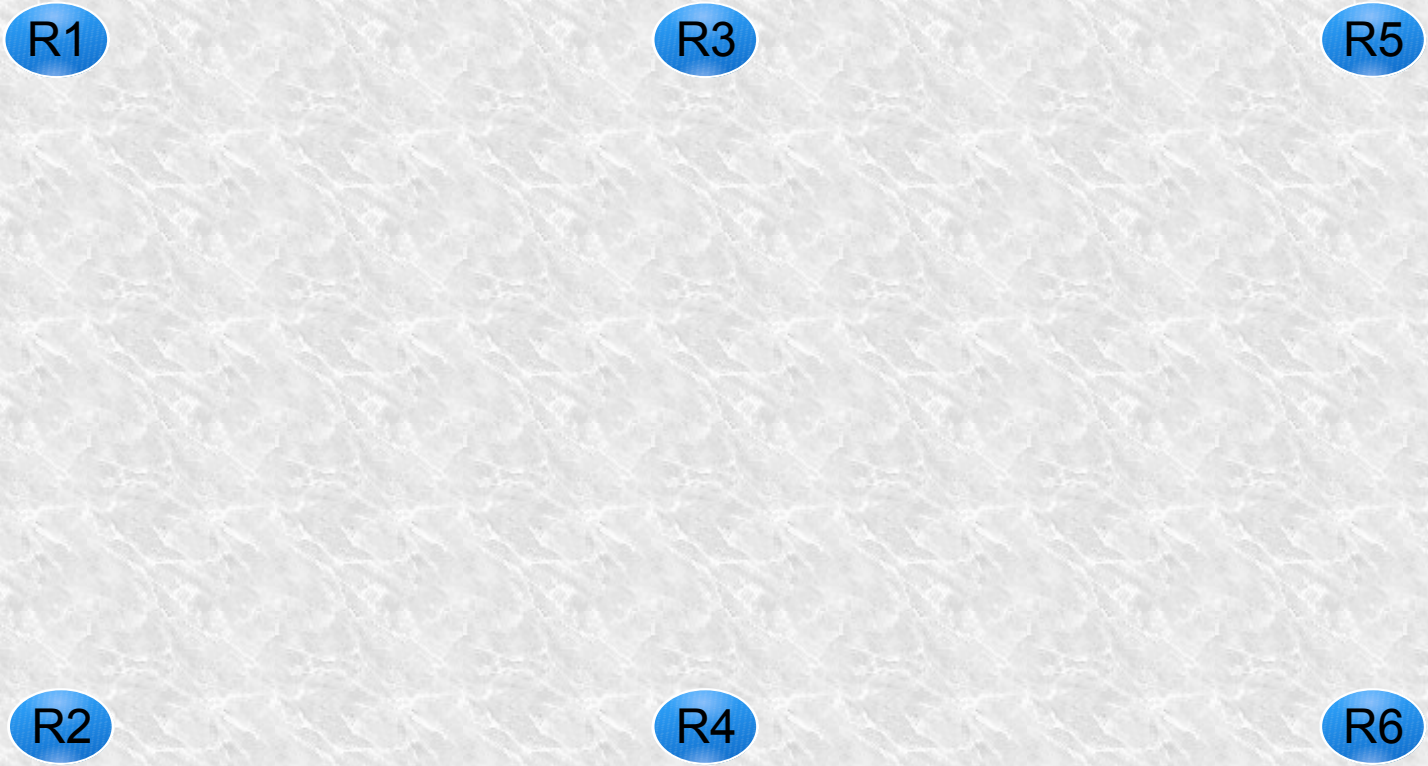
- show ipv6 ospf neighbor
- show ipv6 protocols
- show ipv6 route ospf
- show ipv6 ospf interface brief

“Sfide” nelle Multiaccess Networks

- Le reti multiaccesso possono creare due sfide per l'OSPF per quanto riguarda il flooding delle LSA:
  - Creazione di più adiacenze: le reti Ethernet potrebbero interconnettere molti router OSPF su un collegamento comune. La creazione delle adiacenze di ogni router è inutile e indesiderabile. Ciò porterebbe ad un numero eccessivo di LSA scambiati tra i router sulla stessa rete.
  - Ampio flooding delle LSA: I router configurati con l'OSPF inondano i loro pacchetti di link-state quando l'OSPF viene inizializzato, o quando c'è un cambiamento nella topologia. Queste inondazioni possono diventare eccessive.
- Considerando la lettera “n” come il numero di router, il numero delle adiacenze per numero di router su una rete multiaccesso è dato dalla seguente formula:

$$n (n - 1) / 2$$

Formula n(n-1)/2



OSPF Designated Router

- Il DR (Designated Router) rappresenta la soluzione per la gestione del numero delle adiacenze ed il flooding dei LSA su una rete multiaccesso
- L'OSPF elegge un DR per essere il punto di raccolta e di distribuzione per le LSA inviate e ricevute
- E' inoltre eletto un BDR nel caso in cui il DR si guasti
- I DROTHER: sono i router non DR e non BDR; essi formano una full adjacencies solo con il DR ed il BDR nella rete. Invece di inondare gli LSA a tutti i router della rete, solo i DROTHERs inviano i propri LSA al DR e al BDR utilizzando l'indirizzo multicast 224.0.0.6 (tutti i router DR)
- **NOTA**: 224.0.0.6 è l'indirizzo multicast IPv4 riservato per l'invio verso tutti i DR del protocollo di routing OSPF; FF02::6 è l'indirizzo multicast IPv6 riservato per l'invio verso tutti i DR del protocollo di routing OSPFv3

OSPF Designated Router

- Il DR utilizza l'indirizzo 224.0.0.5 multicast (tutti i router OSPFv2). Il risultato finale è che c'è un solo router che fa tutto l'allagamento di tutti gli LSA nella rete multiaccess.
- **Nota**: L'elezione del DR/BDR si verificano solo nelle reti multiaccesso e non si verificano nelle reti point-to-point.
- Nell'OSPFv3 il DR utilizza l'indirizzo FF02::5 multicast (tutti i router OSPFv3). Il risultato finale è che c'è un solo router che fa tutto l'allagamento di tutti gli LSA nella rete multiaccess.

Verifica del ruolo dei router

- Per verificare il ruolo del router, utilizzare il comando "show ip ospf interface 'nome interfaccia'" dove 'nome interfaccia' è, ad esempio, GigabitEthernet 0/0

GigabitEthernet0/0 is up, line protocol is up

Internet address is 192.168.1.1/24, Area 0

Process ID 1, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DROTHER, Priority 1

Designated Router (ID) 192.168.31.33, Interface address 192.168.1.3

Backup Designated Router (ID) 192.168.31.22, Interface address 192.168.1.2

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:07

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 2, Adjacent neighbor count is 2

Adjacent with neighbor 192.168.31.33 (Designated Router)

Adjacent with neighbor 192.168.31.22 (Backup Designated Router)

Suppress hello for 0 neighbor(s)

Verifica delle adiacenze DR/BDR

- Per verificare le OSPF adjacencies, usare il comando "show ip ospf neighbor"

  R#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.31.22	1	FULL/BDR	00:00:33	192.168.1.2	GigabitEthernet0/0
192.168.31.33	2	FULL/DR	00:00:33	192.168.1.3	GigabitEthernet0/0

- FULL/DR: Il router è completamente adiacente con il DR indicato. Questi due neighbors possono scambiarsi pacchetti Hello, updates, queries, replies e acknowledgments.
- FULL/BDR: Il router è completamente adiacente con il BDR indicato. Questi due neighbors possono scambiarsi pacchetti Hello, updates, queries, replies e acknowledgments.
- A seguire altri possibili valori
- 2-WAY/DROTHER: Il router non-DR e non-BDR ha una neighbor relationship con un altro non-DR e non-BDR. Questi due neighbors si scambiano solo pacchetti Hello.
- FULL/DROTHER: Questo è un router DR o BDR che è completamente adiacente con un router non-DR o BDR. Questi due neighbors possono scambiarsi pacchetti Hello, updates, queries, replies e acknowledgments.

Verifica delle adiacenze DR/BDR

- Lo stato normale per un router OSPF è, di solito, FULL altrimenti è probabile che ci sono problemi; eccezion fatta nel caso in cui lo stato è 2-WAY: questo stato non è sinonimo di problemi.
- Nelle reti multiaccesso, i DROTHER costituiscono solo le full adjacencies con il DR ed il BDR
- I DROTHERs potranno ancora formare una 2-WAY neighbor adjacency con qualsiasi DROTHER che fa parte della rete. Ciò significa che tutti i router DROTHER nella rete multiaccess ricevono ancora i pacchetti Hello da tutti gli altri router DROTHER. In questo modo essi sono a conoscenza di tutti i router della rete. Quando due router DROTHER formano una neighbor adjacency, il neighbor state mostrato sarà 2-WAY/DROTHER

Elezione del DR e del BDR

- I router della rete eleggono il router con la priorità dell'interfaccia più alta come il DR. Il router con la seconda priorità dell'interfaccia più alta viene eletto come il BDR
- La priorità va da 0 a 255; un valore più alto della priorità offre maggiori possibilità al router di diventare DR
- Se impostata a 0 il router non è in grado di diventare DR
- La priorità predefinita delle interfacce di trasmissione multiaccesso è 1.
- Se le priorità delle interfacce sono uguali, allora il router con il più alto router ID viene eletto DR. Il router con il secondo più alto router ID è il BDR
- **Nota**: le interfacce seriali hanno priorità predefinite impostate a 0, quindi, non eleggono DR e BDR.

Elezione del DR e del BDR

- Il processo di elezione richiede solo pochi secondi. Se tutti i router della rete multiaccesso non hanno terminato l'avvio, è possibile che un router con un router ID più basso diventi il DR
- Se un nuovo router con priorità superiore o con un router ID più grande viene aggiunto alla rete dopo l'elezione del DR e del BDR, il router appena aggiunto non assume il ruolo DR o BDR. Questo perché tali ruoli sono già stati assegnati. L'aggiunta di un nuovo router non avvia un nuovo processo elettorale.
- Dopo aver eletto il DR, questo resta il DR fino a quando si verifica uno dei seguenti eventi:
  - Il DR si guasta
  - Il processo OSPF sul DR fallisce o viene arrestato
  - L'interfaccia multiaccess sul DR fallisce o viene arrestata

Elezione del DR e del BDR

- Se il DR si guasta, il BDR è promosso automaticamente a DR
- Dopo che un BDR viene promosso a DR, una nuova elezione BDR si verifica ed il DROTHER con la priorità più alta o con il router ID più grande viene eletto come il nuovo BDR

OSPF priority

- E' possibile influenzare il processo di elezione del DR e del BDR attraverso le configurazioni.
- Se le priorità delle interfacce sono uguali su tutti i router, il router con il più alto router ID viene eletto DR. È possibile configurare il router ID per manipolare l'elezione DR/BDR. Tuttavia, questo processo funziona solo se c'è un piano rigoroso per impostare il router ID su tutti i router. In reti di grandi dimensioni, questo può essere ingombrante.
- Invece di far valere il router ID, è meglio controllare le elezioni stabilendo le priorità dell'interfaccia. Le priorità sono un valore specifico per l'interfaccia, il che significa che fornisce un migliore controllo su una rete multiaccesso. Questo permette ad un router di essere il DR in una rete e un DROTHER in un'altra.

OSPF priority

- Per impostare la priorità di un'interfaccia, utilizzare i seguenti comandi:
  - **ip ospf priority** '*valore*': comando di interfaccia OSPFv2
  - **ipv6 ospf priority** '*valore*': comando di interfaccia OSPFv3
  - '*valore*': 0-255
- Se la priorità dell'interfaccia è configurata dopo che l'OSPF è stato abilitato, l'amministratore deve arrestare il processo OSPF su tutti i router, e quindi riattivare il processo OSPF, per forzare una nuova elezione DR/BDR.
- L'elezione OSPF può essere rinegoziata mediante uno dei seguenti metodi:
  - Shutdown delle interfacce del router e poi ri-abilitarle iniziando con il DR, poi con il BDR, e poi con tutti gli altri router.
  - Resettare il processo OSPF utilizzando il comando "**clear ip ospf process**" in privileged EXEC mode su tutti i router

Propagazione della default static route

- Per propagare una default route, l'edge router deve essere configurato con:
  - Una default static route utilizzando il comando **ip route 0.0.0.0 0.0.0.0** *{ip-address* | *exit-intf}*
  - Il comando **default-information originate** nella modalità di configurazione del router. Ciò indica all'edge router di essere la fonte delle informazioni sulla default route e di diffondere la default static route negli updates OSPF.

Verifica della default static route

- Per verificare le impostazioni della default route utilizzando il comando **show ip route**
- Comando dato su un non edge router

```
R3#show ip route ospf
<parte dell'output è omesso>
O       172.16.1.0 [110/65] via 192.168.10.5, 00:01:33, Serial0/0/0
O*E2  0.0.0.0/0 [110/1] via 192.168.10.9, 00:01:33, Serial0/0/1
```

- La route source è **O*E2**, che sta a significare che è appresa con l'OSPF. L'asterisco indica che la rotta è una buona candidata per essere la route predefinita. La designazione E2 identifica che è un external route (percorso esterno).

Propagazione e verificadella default static route per l'OSPFv3

- Per propagare una default route, l'edge router deve essere configurato con:
  - Una default static route utilizzando il comando **ipv6 route ::/0** *{ ipv6-address* | *exit-intf}*
  - Il comando **default-information originate** nella modalità di configurazione router. Ciò indica ad R2 di essere la fonte delle informazioni sulla default route e di diffondere la default static route negli updates OSPF.
- Per verificare se la default static route è stata propagata utilizzando il comando **show ipv6 route**
- **Nota**: a differenza della tabella di routing IPv4, l'IPv6 non utilizza l'asterisco per indicare che il percorso è un buon candidato per la route predefinita. (O*E2 → OSPFv2; OE2 → OSPFv3)

FINE-TUNING OSPF INTERFACES

- Gli intervalli OSPF Hello and Dead sono configurabili direttamente sull'interfaccia. Gli intervalli OSPF devono corrispondere altrimenti le neighbor adjacency non si verificano.
- Il comando per verificare questi valori è **show ip ospf interface** *nome_interfaccia*
- **Nota**: Gli intervalli predefiniti degli Hello e Dead sono basati sulle migliori pratiche e dovrebbero essere modificati solo in rare situazioni.
- Gli Intervalli OSPF Hello e Dead possono essere modificati manualmente utilizzando i seguenti comandi in modalità di configurazione interfaccia:
  - **ip ospf hello-interval** *seconds*
  - **ip ospf dead-interval** *seconds*

FINE-TUNING OSPF INTERFACES

- Utilizzare i comandi **no ip ospf hello-interval** e **no ip ospf dead-interval** per reimpostare gli intervalli ai valori predefiniti.
- Comandi simili per l'Ipv6:
  - **ipv6 ospf hello-interval** *seconds*
  - **ipv6 ospf dead-interval** *seconds*
  - utilizzare i comandi **no ipv6 ospf hello-interval** e **no ipv6 ospf dead-interval** per reimpostare gli intervalli ai valori predefiniti.
- Quando viene modificato l'intervallo Hello, Cisco IOS modifica automaticamente l'intervallo Dead a quattro volte l'intervallo Hello

Sicurezza nell'OSPF

- Il ruolo del router in una rete è così cruciale che essi sono spesso il bersaglio di attacchi di rete.
- In generale, i sistemi di routing possono essere attaccati interrompendo i routing peers o falsificando le informazioni veicolate all'interno del protocollo di routing.
- Le conseguenze nell'aver falsificato informazioni di routing sono:
  - Reindirizzare il traffico per creare routing loops
  - Reindirizzamento del traffico in modo che possa essere monitorato su un link insicuro
  - Reindirizzare il traffico per disfarsene

  Per mitigare gl attacchi ai protocolli di routing si può configurare l'OSPF authentication.

Mettere in sicurezza gli aggiornamenti di routing

- Quando la neighbor authentication viene configurata su un router, il router autentica la fonte di ogni pacchetto di routing update che riceve. Ciò si ottiene mediante lo scambio di una chiave di autenticazione (talvolta chiamata password) in cui è noto sia il router che inoltra e sia il router che riceve.
- Per scambiare routing update information in modo sicuro, abilitare l'OSPF authentication

Mettere in sicurezza gli aggiornamenti di routing

- L'OSPF supporta 3 tipi di autenticazione:
  - Null: è il metodo predefinito e significa che nessuna autenticazione viene utilizzata per l'OSPF.
  - Simple password authentication: E' indicata anche come plaintext authentication perché la password nell'update viene trasmessa in chiaro attraverso la rete. E' considerato un legacy method of OSPF authentication. (legacy = eredità)
  - MD5 authentication: Questo è il metodo di autenticazione più sicuro e consigliato. L'autenticazione MD5 fornisce maggiore sicurezza, perché la password non viene mai scambiata tra i peers. Invece è calcolata utilizzando l'algoritmo MD5. I risultati che corrispondono autenticano il mittente.
- **Nota**: L'OSPFv3 si basa interamente su IPSec per proteggere le comunicazioni tra i neighbors utilizzando il comando **ipv6 ospf authentication ipsec spi** in modalità di configurazione interfaccia.

Configurazione dell'OSPF MD5 Authentication

- L'autenticazione MD5 può essere attivata a livello globale (per tutte le interfacce) o singolarmente su una o più interfacce
- Per abilitare l'autenticazione MD5 OSPF a livello globale, configurare:
  - **ip ospf message-digest-key** *key* **md5** *password* - comando in modalità di configurazione interfaccia.
  - **area** *area-id* **authentication message-digest** comando in modalità di configurazione del router.
- Per abilitare l'autenticazione MD5 OSPF su una singola interfaccia configurare:
  - **ip ospf message-digest-key** *key* **md5** *password* - comando in modalità di configurazione interfaccia.
  - **ip ospf authentication message-digest** comando in modalità di configurazione interfaccia.

Configurazione dell'OSPF MD5 Authentication

- L'autenticazione MD5 OSPF per-interfaccia e l'autenticazione MD5 OSPF globale possono essere utilizzate sullo stesso router. Tuttavia, l'impostazione dell'interfaccia sostituisce l'impostazione globale. La password di autenticazione MD5 non devono essere la stessa per tutta una zona, tuttavia, esse devono essere uguali tra i neighbors.
- Il comando per verificare l'autenticazione MD5 è **show ip ospf interface** *interface_id*
- Nelle due righe finali del comando troveremo la dicitura:

  Message digest authentication enabled

  Youngest key id is 1

TROUBLESHOOTING SINGLE-AREA OSPF

- L'OSPF è un protocollo di routing comunemente implementato e usato in grandi reti aziendali. La risoluzione dei problemi relativi allo scambio di informazioni di routing è una delle competenze più essenziali per una rete professionale che è coinvolta nella realizzazione e nella manutenzione di grandi reti aziendali con routing che utilizzano l'OSPF come IGP.
- I problemi con la formazione delle adiacenze OSPF sono:
- Le interfacce non sono sulla stessa rete.
- I tipi di rete OSPF non corrispondono.
- Gli OSPF Hello e Dead Timer non corrispondono.
- L'interfaccia verso il neighbor è configurata erroneamente come passiva.
- C'è un comando **network** OSPF mancante o errato.
- L'autenticazione non è configurata correttamente.

TROUBLESHOOTING SINGLE-AREA OSPF

- Per risolvere i problemi OSPF, è importante capire come un router OSPF attraversa i diversi stati di OSPF quando vengono stabilite le adiacenze.
- Quando si hanno problemi con gli OSPF neighbors, bisogna essere consapevoli del fatto che gli stati FULL o 2WAY sono normali. Tutti gli altri stati sono transitori, cioè, il router non dovrebbe rimanere in quegli stati per periodi di tempo prolungati

Comandi che aiutano nella risoluzionedei problemi

- **show ip protocols**: usato per verificare le informazioni vitali di configurazione OSPF, compreso il process ID OSPF, il router ID, le reti che il router pubblicizza, i neighbors da cui il router sta ricevendo gli updates, e la distanza amministrativa di default, che è di 110 per OSPF.
- **show ip ospf neighbor**: usato per verificare che il router ha formato un adiacenza con i suoi router vicini. Visualizza il router ID dei neighbors, la priority del neighbor, lo stato OSPF, il Dead timer, l'indirizzo IP dell'interfaccia del neighbor, e l'interfaccia attraverso la quale il neighbor è accessibile. Se il router ID del neighbor router non viene visualizzato, o se non viene visualizzato sullo stato di FULL o 2WAY, i due router non hanno costituito un adiacenza OSPF. Se due router non stabiliscono un'adiacenza, non saranno scambiate informazioni di link-state. I database di link-state incompleti possono causare alberi SPF imprecisi e tabelle di routing imprecise. I percorsi di reti verso la destinazione non possono esistere o non può essere il percorso ottimale.

Comandi che aiutano nella risoluzionedei problemi

- **show ip ospf interface**: usato per visualizzare i parametri OSPF configurati su un'interfaccia, come il process ID OSPF a cui l'interfaccia è assegnata, il costo dell'interfaccia, e gli intervalli di Hello e di Dead. Aggiungendo al comando il nome dell'interfaccia e il numero l'output sarà visualizzato per una specifica interfaccia.
- **show ip ospf**: usato per esaminare il process ID OSPF ed il router ID. Inoltre, questo comando visualizza le informazioni dell'area OSPF, così come l'ultima volta che l'algoritmo SPF è stato calcolato.
- **clear ip ospf** *[process-id]* **process**: Usato per ripristinare le neighbor adjacencies OSPFv2.

End of lesson